JUDGE BATTS

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

'11 CIV 7086

KRISTINA AND STEVEN ORMAN, Individually and on Behalf of All Others Similarly Situated,	:	**Case No.**
Plaintiffs,	:	
-against-	:	**CLASS ACTION COMPLAINT**
CITIGROUP, INC., CITICORP USA INC., and CITIBANK, N.A.,	:	
Defendants.	:	**Jury Trial Demanded**

Plaintiffs Kristina and Steven Orman bring this class action lawsuit on behalf of themselves and all others similarly situated, upon personal knowledge as to the facts pertaining to them and upon information and belief as to all other matters, based on investigation of their counsel, against defendants Citigroup, Inc., ("Citigroup"); Citicorp USA Inc., ("Citicorp"); and Citibank, N.A. ("Citibank") (collectively hereinafter "Defendants" or "Citi"), and state as follows:

NATURE OF ACTION

1. This is a consumer class action for damages and injunctive relief arising from Defendants' negligent, deceptive, and unlawful conduct in securing card holders' sensitive financial information.

2. On or about May 10, 2011, Citi disclosed that it suffered a security breach (the "Breach") affecting more than 360,000 customers exposed to hackers.

3. Defendants' debit and credit card service ("the Service") was inadequately secured against intrusion and breach of security into extremely sensitive customer financial

information, causing interruption of the use of the Service, damage to the credit ratings of, and financial loss to debit and credit card holders (together "Card Holders").

4. Further, Defendants keep and maintain a database of all Card Holders, their account records and statements, and any financial information the Card Holder has provided to Defendants. All financial records pertaining to bank records were potentially stolen because of Defendants' lax security policies and procedures, thereby injuring Card Holders.

5. Defendants have taken no steps that adequately or effectively protect Card Holders against illegal use of the Card Holders' sensitive and extensive financial records since the Breach.

6. Defendants have made no attempt to compensate injured Card Holders for adequate monitoring or to aid Card Holders to take adequate action to repair the harm to the credit ratings of Card Holders as the result of Defendants' totally inadequate security in relation to monitoring highly sensitive data, as is required under contract and various state laws.

7. The Defendants have not disclosed how they have come to their stated conclusion that "more sensitive info like social security numbers, birth dates, card expiry dates and CVV card security codes were not compromised."

PARTIES

8. Plaintiffs Kristina and Steven Orman ("Plaintiffs" or the "Ormans") are residents of Northport, New York. The Ormans are the victims of identity theft ("ID Theft") as the result of the negligence of Defendants in securing Card Holders' sensitive financial information.

9. The Ormans have bank and credit card accounts with Citi which were breached and consequently they suffered a financial loss when money was stolen from their bank account.

Moreover, due to Defendants' failure to adequately protect the Ormans' financial information, credit accounts were opened by third parties in the Ormans' name without their knowledge or consent, and retail purchases were made by third parties on their existing credit cards.

10. Defendant Citigroup is a global financial services holding company whose businesses provide consumers, corporations, governments, and institutions with a broad range of financial products and services, including consumer banking, credit cards, corporate and investment banking, securities brokerage, and wealth management. Citigroup has approximately 200 million customer accounts and does business in more than 160 countries. Citigroup was incorporated in 1988 in the State of Delaware.

11. Defendant Citicorp is a business segment of Citigroup and operates a nationally chartered bank. The business of Citicorp includes retail banking and Citi-branded cards. Citicorp is incorporated in Delaware with its principal place of business in New York, New York.

12. Defendant Citibank represents the consumer banking operations of Citigroup. Citibank has more than 1,000 branches in about a dozen US states. Citibank provides standard banking fare such as deposit accounts, credit cards, and loans to consumers. Effective July 1, 2011, Citibank (South Dakota) N.A., merged into Citibank. Citibank's corporate headquarters are located at 399 Park Avenue, New York, New York 10022.

VENUE AND JURISDICTION

13. Venue in this Court is proper because Defendants' principal executive offices are located in this Judicial District, and because a substantial part of the acts or omissions giving rise to the claims in this action occurred in this Judicial District.

14. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (a) the class has more than 100 members, (b) at least one of the members of the proposed class is a citizen of a state other than New York, and (c) the total amount in controversy exceeds $5 million exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendants as Defendants' principal executive offices are located in this Judicial District; a substantial portion of the wrongdoing alleged in this Complaint took place in this District; Defendants are authorized to do business in this District; and Defendants have sufficient minimum contacts with this District, and/or otherwise intentionally avail themselves of the markets in this District through the promotion, marketing, and sales of its Products and the Service in this District so that the exercise of personal jurisdiction by this Court complies with judicial notions of fair play and substantial justice.

GENERAL ALLEGATIONS

Defendants' Account Data Security

16. A credit card is a small plastic card issued to users as a system of consumer payment. It allows its holder to buy goods and services based on the holder's promise to pay for these goods and services. A debit card provides the cardholder electronic access to his or her bank accounts at a financial institution.

17. Defendants claim to be the world's largest credit card company with hundreds of millions of credit cards worldwide and with 21 million customers in North America alone, according to recently filed financial documents.

18. In connection with the Service, Defendants advertise and claim to offer various benefits, including "Identity Theft Solutions" and "Account Security." On the Defendants' corporate website on a page entitled https://creditcards.citi.com/services/, the following benefits are listed:

> **Citi® Identity Theft Solutions**
> Let us educate and assist you in taking the steps necessary to reestablish your credit and reclaim your identity in the case of ID theft.
>
> **Account Security**
> As a leader in the prevention and detection of credit card fraud, Citi® is constantly safeguarding and protecting you and your account.
>
> **Citibank® Services**
> Your Citi® credit card entitles you to a wide range of Citibank® services. Get 24/7 customer service, additional cards, worldwide credit card acceptance and much more.
>
> **Money Management Services**
> Citi® credit cards come with money management services that help you keep your finances in check, whether for personal or business needs.
>
> **Travel Services**
> Your Citi® credit card has you covered when you travel. Benefit from auto rental insurance coverage and discounts from Hertz.
>
> **Convenience Services**
> Realize the built-in convenience of having a Citi® credit card – select a due date for bill payment and make purchases with tap-and-go convenience.
>
> **Recurring Bill Payments**
> Use your Citi® credit card to automatically pay vendors such as your cable, phone, or utilities provider.
>
> **Citi MobileSM**
> Manage your Citi credit card accounts anywhere, anytime using our free mobile banking services

Defendants' Poorly Secured Website

19. Defendants' purported concern for account security does not appear to extend

beyond Citi's corporate website. In an interview with Reuters in April 2011, Citigroup global enterprise payments head Paul Galant expressed a somewhat relaxed view on the topic: "Security breaches happen, they're going to continue to happen . . . the mission of the banking industry is to keep the customer base safe and customers *feeling* secure about their financial transactions and payments." (Emphasis added).

20. Defendants' card holder database contains highly sensitive information including, but not limited to, account holders' names, credit card numbers, contact information, social security numbers, dates of birth, credit card expiration dates, and credit card security codes called CVV codes.

21. On June 11, 2011, INDUSTRY LEADERS MAGAZINE reported that in the wake of the Breach, Sheila C. Bair, head of the Federal Deposit Insurance Corporation, urged banks to strengthen their authentication procedures when customers access their financial accounts online.

22. In a June 13, 2011 article titled "Thieves Found Citigroup Site an Easy Entry," THE NEW YORK TIMES likened Defendants' customer website to a thief's dream: "Think of it as a mansion with a high-tech security system — but the front door wasn't locked tight."

23. In a website that guards sensitive information, strong protection against intrusion is vital and in some cases required by law. Strong passwords are one method of slowing hackers.

24. According Microsoft Safety & Security Center, strong passwords are important protections to help consumers have safer online transactions because they are harder for third parties to hack. Strong passwords are typically 14 characters or more: the greater the variety of characters in the password, the stronger it is. Websites that don't require strong passwords

make a hacker's job infinitely easier.

25. Citi employed a system of generating web based financial information that used each customer's account number as part of the web address for that customer's page. A Citi customer would log into the Citi website with a user name and password. Citi would then generate and display the customer's account information. Once the account was accessed the customer's account number would be displayed as part of the web address.

26. In the Breach, hackers logged into that part of the website using a valid account. Once logged in, they were able to access other accounts by substituting other account numbers in the text of the address bar.

27. Once a hacker had accessed a customer's account, the hacker could use simple "brute force" methods to access financial account data. One reason that Defendants allowed this to happen was cost. A brute force data intrusion relies upon a weakness in the given security system. If one part of a security system is known, hackers write programs that substitute millions of possible answers to the unknown part of the system, until the hacker finds the right data.

28. The INTERNATIONAL BUSINESS TIMES has noted, "Banks and credit card companies have tolerated a certain amount of fraud in their systems because the cost of additional security would not justify the potential savings."

29. Defendants were willing to accept security risks to save money for the bank while exposing the customer to huge financial risk.

The Breach, Resulting Stolen Information, and Citi's Cover-up

30. On or about May 10, 2011, Citi claims that it discovered that their Online Web

Portal had been accessed by a third party during the Breach.

31. According to Defendants, the Breach was "immediately rectified" and by May 24, 2011, Defendants claimed that they had confirmed the full extent of information accessed by hackers via the Breach. Citi did not begin to notify customers whose accounts were compromised until June 3, 2011.

32. In fact, the Breach had begun months before it was discovered by Defendants. On June 29, 2011, in an editorial titled "The Cloud Darkens," the NEW YORK TIMES reported that Citi failed to notice the hack because Citi did not track patterns of its activity on its credit card site.

33. Citi has yet to announce the true date of when the Breach started and how Citi's website was hacked.

34. According to Citi, only some of its credit card customers' information had been accessed while other customers' accounts, including checking accounts, were not compromised. This proved to be untrue, as both credit card and checking account customers' information was accessed by hackers during the Breach.

35. Citi stated that during the Breach "[t]he customers' account information (such as name, account number and contact information, including email address) was viewed. However, data that is critical to commit fraud was not compromised: the customers' social security number, date of birth, card expiration date and card security code (CVV)."

36. Whatever the case, Citi waited until June 9, 2011 - nearly one month after purportedly discovering the Breach - to alert customers who, in Citi's view, were not impacted by the Breach.

37. Ultimately, Citi acknowledged that a total of 360,083 North American Citi-branded credit card accounts were affected and 217,657 accounts were reissued credit cards along with a notification letter. According to Citi, "Some accounts were not re-issued credit cards if the account is closed or has already received new credit cards as a result of other card replacement practices. These accounts continue to receive heightened monitoring for suspicious activity."

Citi Allowed Customers' Money, Personal, And Banking Information To Be Stolen

38. On June 9, 2011, REUTERS reported that although Citi had not disclosed how the Breach occurred, it did state that:

> [T]he names of customers, account numbers and contact information, including email addresses, were viewed in the breach, which the FINANCIAL TIMES said was discovered by the bank in early May. However, Citi said other information such as birth dates, social security numbers, card expiration dates and card security codes CVV were not compromised.

39. Citi has also misstated the extent of the accounts affected by the Breach. Citi has consistently maintained that credit card customers were the only accounts affected. However, in a June 9, 2011 article titled "Citi Admits Customer Data At Risk After Breach", the FINANCIAL TIMES reported, "Citi said the breach affected credit card accounts only, but several people that the [FINANCIAL TIMES] spoke to said their debit cards were compromised. These people said they did not learn of the problem until they tried to use their cards at the weekend and had the transactions denied."

Customers' Stolen Money

40. Initially, Citi assured customers and the public that information accessed by hackers in the Breach would not lead to fraud.

41. As facts emerged, Defendants confirmed that hackers had in fact committed fraud using information stolen during the Breach. Citi reported that $2.7 million was stolen from 3,400 customers when their information was leaked.

Need for Third Party Credit Monitoring

42. Citi directs customers to use self help and monitor their accounts themselves to ensure that they don't fall victim to fraud. Citi advises customers to review their account statements and to report any suspicious or unauthorized charges to Citi.

43. Defendants continue to provide inadequate security to protect the sensitive data of Plaintiffs and members of the putative class. Defendants' inadequate security measures have left and continue to leave Citi customers vulnerable to ID theft.

44. Because of Defendants' lax security measures, Plaintiffs and the proposed class are also open to scams wherein third parties attempt to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity.

45. In a June 22, 2011 article, entitled "Citigroup Hack Prompts Bank Reg Debate," published in THE STREET, Marc Rotenburg, president of Electronic Privacy Information Center, stated that the financial services industry, including Citi, deserved some of the blame for identity theft concerns because the credit granting system and electronic payment mechanisms were designed in a way that makes committing fraud easy. "The industry favors convenience over security because tolerating some identity theft is more often profitable for companies." Rottenberg went on to point out that the victims of Citi's lax security would continue to suffer damages as customer accounts are now prone to what are called phishing attacks: "Spear phishing is a more effective and targeted version of phishing as the source of the e-mails sent to

the potential victims comes from a supposedly trusted or known source. In instances such as this, consumers should be notified so that they can take proper precautions against future attacks and possible fallout from the data breach."

46. On June 25, 2011, BLOOMBERG NEWS reported that hackers could commit fraud with the data Citi acknowledged was stolen by matching the information they accessed in the Citi Breach with information stolen elsewhere.

47. In an article entitled "Data Breaches Bring Back Failed Legislation From the Dead," published in INFORMATION MANAGEMENT on June 22, 2011, technology consultant Judith Hurtwitz of Hurwitz and Associates opined that although consumers may have some liability protections against data theft, there are other dangers from data breaches that could be mitigated by extra protection: "[data breaches are] not just a compromise of a specific payment, [they] compromise[] someone's identity."

48. In fact numerous security advisers and news outlets have warned customers not to trust Defendants' security and suggest that they take matters into their own hands. On June 9, 2011, after Defendants first publically announced the Breach, Chester Wisniewski, a senior security advisor at security firm Sophos, issued the following advice to Defendants' customers:

> Customers affected by this incident should be on high alert for scams, phishing and phone calls purporting to be from Citibank and their subsidiaries. While Citi customers aren't likely to have fraudulent charges against their accounts as a result of this breach, they are likely to encounter social engineering attempts to enable further crime. Considering that the attackers have your name, account number and other sensitive information they are able to provide a very convincing cover story to victims.

Disclosure

49. On June 9, 2011, Defendants first publicly announced that 210,000 Citi Credit customers' accounts had been hacked. Citi denied that Citi Debit accounts had been compromised.

50. According to Citi, the Breach occurred in early May 2011. A June 14, 2011 FINANCIAL TIMES article entitled "Officials Press Citi For Info On Hacking Attack," noted that "Citi began notifying about 200,000 customers and reissuing cards last week."

51. On June 15, 2011, Citi admitted that the initial information it provided to news outlets that the Breach only affected 210,000 accounts was a vast understatement: "[b]y May 24, we confirmed the full extent of information accessed on 360,069 accounts. An additional 14 accounts were confirmed subsequently."

52. Defendants blamed the delayed announcement on the fact that Citi was continuing to investigate the Breach and "developing notification packages including customer letters and manufacturing replacement cards, as well as preparing our customer service teams."

Citi's Delayed Announcement Violated State Security and Consumer Statutes

53. California Civil Code Sections 1798.82 and 1798.2, *inter alia*, regulate disclosure of computer data. The statutes require "a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

54. In general, most state laws follow the basic tenets of California's consumer data protection law: companies must immediately disclose a data breach to customers, consumer protection agencies, and appropriate state entities, usually in writing.

55. Similar laws exist in Alaska, Iowa, South Carolina, Virginia, West Virginia, and Washington D.C., and require disclosure of a breach "without unreasonable delay."

56. Massachusetts law requires that the attorney general be notified of a data breach. Defendants did send a letter to the Massachusetts' attorney-general on June 10, 201, but only after widespread news coverage about the Breach on June 9, 2011. The FINANCIAL TIMES reported, "According to the Citi letter, 7,904 Massachusetts residents were affected, an official said."

57. In contrast, Defendants did not provide any information concerning the Breach to the attorney general of Connecticut, where no such notice is required, until after the attorney general sent a letter on June 13, 2011 to Citi requesting details about the Breach. Subsequently, as noted above, on June 15, 2011, Citi announced that in fact more than 360,000 accounts had been compromised, 41% more than reported just five days before.

58. Upon information and belief, Defendants similarly did not notify any of the Card Holders in states that require such notification.

59. Defendants' delay in disclosing the Breach not only violated state laws, but made it impossible for Plaintiffs and the putative Class to mitigate their financial and other harm through self-help or third party assistance.

The Orman Plaintiffs' Experience

60. Due to the Defendants' actions, the Ormans suffered direct financial loss. Third parties accessed the Ormans' personal/financial information during the Breach. The third party hackers then used the stolen data to empty the Ormans' checking account. A day after Ms. Orman's pay check was deposited, the money was stolen from her checking account.

61. Citi acknowledged over the phone to Ms. Orman that money was stolen from the Ormans' Citi checking account due to "Citi operators neglect in asking for a password or other identifying questions."

62. The Ormans' accounts were inundated with credit checks from credit rating companies including TransUnion, Experian, and Equifax, including inquiries made upon the request of Defendants. Thus the ID theft that resulted from the fraudulent activity caused by Defendants' negligence has damaged the Ormans' credit rating.

63. Defendants themselves rejected the Ormans' recent request for an increase in overdraft protection by citing "too many credit inquiries" on the account.

64. The Ormans have been forced to spend time and effort to protect both their money and their credit rating.

65. Citi claims to have tightened client data security to safeguard against future fraud. Defendants' website claims, "[W]e continue to monitor customer service and communication channels and take every necessary action to ensure our customers are cared for."

66. In fact, the Plaintiffs' experience is to the contrary. Citi's policy states that when a customer who has called Citi is transferred from the representative who answered the call to a second representative, the second representative must repeat the procedure of asking the

customer identifying questions. However, when Ms. Orman recently called Citi, and was transferred from one representative to another, this procedure was not followed so Citi did not know for certain that they were actually speaking with a legitimate account holder.

CLASS ACTION ALLEGATIONS

67. Plaintiffs bring this action pursuant to Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of themselves and a Class defined as follows:

> All Card Holders whose information was stolen in the Breach from early May, 2011 until such date that clarifies the extent of Defendants' Breach.
>
> Excluded from the Class are (i) Defendants, any entity in which Defendants have a controlling interest or which has a controlling interest in Defendants, and Defendants' legal representatives, predecessors, successors, assigns, and employees and (ii) the judge and staff to whom this case is assigned, and any member of the judge's immediate family.

68. Plaintiffs are members of the Class that they seek to represent. Members of the Class can be identified using Defendants' records of Card Holder information, and other information that is kept by Defendants in the usual course of business and/or in the control of Defendants. Class members can be notified of the class action through publication on Card Holder websites, direct mail, and direct e-mailings to address lists maintained in the usual course of business by Defendants.

69. Class members are so numerous that their individual joinder is impracticable. The precise number of the class members is unknown to Plaintiffs, but it is clear that the number greatly exceeds the number to make joinder impossible.

70. Common questions of law and fact predominate over the questions effecting only individual Class members. Some of the common legal and factual questions include:

a. Whether Defendants' Cards and Service were defectively designed, marketed, and secured;

b. Whether Defendants knew or should have known that the Service was defectively designed, marketed, and secured;

c. Whether Defendants knowingly concealed the defective nature of the Service and the Breach;

d. Whether Defendants disclosed the Breach of financial information to Card Holders in a timely manner;

e. Whether Defendants engaged in illegal business practices by failing to monitor or sufficiently offer third party credit monitoring without charging the Class members;

f. Whether Defendants misrepresented the safety, security, and usefulness of the Service, including storage of Card Holder financial information;

g. Whether, by the misconduct set forth herein, Defendants violated consumer protection statutes and/or false advertising statutes and/or state deceptive business practices statutes;

h. Whether, by the misconduct set forth herein, Defendants breached contracts with Card Holders;

i. Whether, by the misconduct set forth herein, Defendants violated the common laws of negligent misrepresentation and unjust enrichment;

j. Whether, by the misconduct set forth herein, Defendants breached their duty of good faith and fair dealing; and

k. The nature and extent of damages and other remedies to which the conduct of Defendants entitles the class members.

71. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by the class members. Similar or identical defective designs and practices, statutory, and common law violations, deceptive business practices, and defective online access and the Service are involved. Individual questions, if any, pale by comparison to the numerous common questions that dominate.

72. The injuries sustained by the Class members flow from a common nucleus of operative facts, *i.e.* Defendants' defective Services and the Breach.

73. The class members have been damaged by Defendants' misconduct as detailed *supra* including but not limited to the financial loss resulting from Citi's delayed notification of the Breach and false assurances of increased security protection that Defendants touted as a feature of their Products and Services. The delay and false assurances precluded class members from promptly using third party credit monitoring services.

74. Plaintiffs' claims are typical of the claims of the other proposed class members. Plaintiffs used Defendants' Service to their detriment and were damaged thereby.

75. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs are familiar with the basic facts that form the basis of the proposed class members' claims. Plaintiffs' interests do not conflict with the interests of the other class members that they seek to represent. Plaintiffs have retained counsel competent and experienced in class action litigation and intend to prosecute this action vigorously. Plaintiffs' counsel has successfully prosecuted

complex class actions, including consumer protection class actions. Plaintiffs and Plaintiffs' counsel will fairly and adequately protect the interests of the class members.

76. The class action device is superior to other available means for the fair and efficient adjudication of the claims of Plaintiffs and the proposed class members. The relief sought per individual member of the Class is small given the burden and expense of individual prosecution of the potentially extensive litigation necessitated by Defendants' conduct. Furthermore, it would be virtually impossible for the class members to seek redress on an individual basis.

77. Individual litigation of the legal and actual issues raised by the conduct of Defendants would increase delay and expense to all parties and to the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION
State Identity Theft Protection Laws

78. The Plaintiffs hereby incorporate by reference each paragraph of this Complaint, as if fully set forth herein.

79. The following state statutes require that Citi provide notification of the Breach to customers whose information or identities may be compromised by a security breach, as well as consumer reporting agencies, and/or the State Attorney General:

Alaska:	Alaska Stat. § 45.48.010 *et seq.*;
Arizona:	Ariz. Rev. Stat. § 44-7501;
Arkansas:	Ark. Code § 4-110-101 *et seq.*;
California:	Cal. Civ. Code §§ 1798.29, 1798.82;

Colorado:	Colo. Rev. Stat. § 6-1-716;
Connecticut:	Conn. Gen Stat. 36a-701*et seq.*;
Delaware:	Del. Code tit. 6, § 12B-101 *et seq.*;
Florida:	Fla. Stat. § 817.5681;
Georgia:	Ga. Code §§ 10-1-910 *et seq.*;
Hawaii:	Haw. Rev. Stat. § 487N-2;
Idaho:	Idaho Code Ann. § 28-51-104;
Illinois:	815 Ill. Comp. Stat. 530/1 *et seq.*;
Indiana:	Ind. Code §§ 24-4.9-2-1 *et seq.*, 4-1-11 *et seq.*;
Iowa:	Iowa Code § 715C.1 *et seq.*;
Kansas:	Kan. Stat. 50-7a01-50-7a02;
Louisiana:	La. Rev. Stat. Ann. § 51:3071 *et seq.*;
Maine:	Me. Rev. Stat. tit. 10 §§ 1347 *et seq.*;
Maryland:	Md. Code, Com. Law § 14-3501 *et seq.*;
Massachusetts:	Mass. Gen. Laws 93H § 1 *et seq.*;
Michigan:	Mich. Comp. Laws § 445.72;
Minnesota:	Minn. Stat. §§ 325E.61, 325E.64;
Mississippi:	Miss. Code. Ann. § 75-24-29;
Missouri:	Mo. Rev. Stat. § 407.1500 *et seq.*;
Montana:	Mont. Code §§ 30-14-1704, 2-6-504;
Nebraska:	Neb. Rev. Stat. §§ 87-801-8cy;
Nevada:	Nev. Rev. Stat. 603A.010 *et seq.*;

New Hampshire:	N.H. Rev. Stat. §§ 359-C:19, -C:21;
New Jersey:	N.J. Stat. 56:8-163;
New York:	N.Y. Gen. Bus. Law § 899-aa;
North Carolina:	N.C. Gen. Stat § 75-65;
North Dakota:	N.D. Cent. Code § 51-30-01 *et seq.*;
Ohio:	Ohio Rev. Code §§ 1349.19, 1349.192;
Oklahoma:	74 Okla. Stat. §§ 3113.1, 24-161-166;
Oregon:	Or. Rev. Stat. § 646A.600 *et seq.*;
Pennsylvania:	73 Pa. Stat. § 2303;
Rhode Island:	R.I. Gen. Laws § 11-49.2-1 *et seq.*;
South Carolina:	S.C. Code § 39-1-90;
Tennessee:	Tenn. Code § 47-18-2107;
Texas:	Tex. Bus. & Com. Code § 521.053;
Vermont:	9 Vt. Stat. § 2430 *et seq.*;
Virginia:	Va. Code § 18.2-186.6;
Washington:	Wash. Rev. Code §§ 19.255.010-020, 42.56.590;
West Virginia:	W.V. Code §§ 46A-2A-101 *et seq.*;
Wisconsin:	Wis. Stat. § 134;
Wyoming:	Wyo. Stat. § 40-12-501-502; and
District of Columbia:	D.C. Code § 28- 3851 *et seq.*

80. Defendants claim that they first became aware of the Breach on May 10, 2011. In violation of the afore mentioned state statutes, Defendants failed to timely notify consumers

and the required persons and/or entities of the Breach. Citi waited until June 9, 2011 - nearly one month after purportedly discovering the Breach - to alert the public and other customers who, in Citi's view, were not impacted by the Breach.

81. Moreover, Defendants are not exempt from the statutory requirement to timely notify the required persons/entities.

82. To the extent Defendants provided notice to the required persons/entities, the notice was insufficient and invalid because the notice did not conform to the notification requirements mandated by each state. As the result of Defendants' conduct, Plaintiffs and the Class were harmed.

SECOND CAUSE OF ACTION
Implied Warranty of Merchantability and Fitness for Particular Purpose

83. Plaintiffs hereby incorporate by reference each paragraph of this Complaint, as if fully set forth herein.

84. Defendants warranted that the Services they sold were of merchantable quality. The Defendants are well-known merchants with respect to services of that kind. Plaintiffs and the Class relied on Defendants' skill and ability to furnish suitable services. The Service did not conform to the promise or affirmations of fact made in their advertisements and/or on Defendants' corporate website as to the security of the corporate website and Card Holder data. As the result of Defendants' conduct, Plaintiffs and the Class were harmed.

THIRD CAUSE OF ACTION
Common Law Negligence

85. Plaintiffs hereby incorporate by reference each paragraph of this Complaint, as if fully set forth herein.

86. The Defendants systematically failed to monitor Citi's website security. Defendants failed to use encryption and other common forms of data protection to secure Card Holder data. Defendants did not use adequate hardware firewalls and other network security equipment to safeguard Card Holder financial information and other sensitive Card Holder information. By not using widely accepted and adequate network security, Defendants were negligent in their duty to safeguard Card Holder data. Defendants did not disclose the data breach of financial information to Card Holders in a sufficient or timely manner.

87. As such, some class members were fraudulently billed on credit cards stored with Defendants. With this knowledge, Defendants did not act to cure their breach.

88. Subsequently, Defendants failed to monitor or sufficiently offer third party credit monitoring for no charge to the class members in a timely fashion.

89. As the result of Defendants' conduct, Plaintiffs and the Class were harmed.

FOURTH CAUSE OF ACTION
Breach Of GBL 349 And 350 And The Various Analogous State Consumer And Advertising Laws

90. The Plaintiffs hereby incorporate by reference each paragraph of this Complaint, as if fully set forth herein.

91. Defendants' extension of the Service to Plaintiffs and the Class as described herein constitutes the "conduct of any trade or commerce" within the meaning of N.Y. GBL 349. Defendants, in the normal course of their business, collected Card Holder information while stating that such data would remain private. Defendants misrepresented the safety, security, and usefulness of the Service, including storage of Card Holder financial information.

92. The foregoing acts and conduct of Defendants are deceptive in that they represented to the consumer class that such information would remain secure and/or that Defendants had the technology or policies to secure such information when Defendants did not have such security measures, including but not limited to the failure to encrypt such information in the event that the information would fall into the hands of third parties.

93. By warranting that the Service was secure, Defendants violated consumer protection statutes and/or false advertising statutes and/or state deceptive business practices statutes and by their deceptive actions, Plaintiffs and the Class were harmed.

94. Defendants' actions, as complained of herein, constitute unfair competition or unfair, unconscionable, deceptive, or fraudulent acts or practices in violation of the various state consumer protection statutes listed below:

Alabama:	Ala. Code 8-19-1 *et seq.*;
Alaska:	Alas. Code 45.50.471 *et seq.*;
Arizona:	Ariz. Code 44-1521 *et seq.*;
Arkansas:	Ark. Code 4-88-101 *et seq.*;
California:	Cal. Bus. & Prof. Code §§ 17200 *et seq.*, §§ 17500 *et seq.*;
Connecticut:	Conn. Code 6-1-105 *et seq.*;
Colorado:	Colo. Rev. Stat. Ann. 42-110b *et seq.*;
Delaware:	6 Del. Stat. Code 2511 *et seq.*;
District of Columbia:	D.C. Code 28-3901 *et seq.*;
Florida:	Fla. Stat. 501.201 *et seq.*;
Georgia:	Ga. Stat. 10-1-392 *et seq.*;

Hawaii:	Haw. Rev. Stat. 480-2 *et seq.*;
Idaho:	Idaho Code 48-601 *et seq.*;
Illinois:	815 Ill. Comp. Stat. 505/1 *et seq.*;
Indiana:	Ind. Code Ann. 24-5-0.5-1 *et seq.*;
Iowa:	Iowa Code 714.16 *et seq.*;
Kansas:	Kan. Stat. 50-623 *et seq.*;
Kentucky:	Ky. Rev. Stat. 367.110 *et seq.*;
Louisiana:	La. Rev. Stat. 51:1401 *et seq.*;
Maine:	5 Me. Rev. Stat. 207 *et seq.*;
Maryland:	Md. Code, Com. Law 13-101 *et seq.*;
Massachusetts:	Mass Gen. L. Ann. 93A *et seq.*;
Michigan:	Mich. Stat. 445.901 *et seq.*;
Minnesota:	Minn. Stat. 325F.68 *et seq.*;
Mississippi:	Miss. Code Ann. 75-24-3,5,15\ *et seq.*;
Missouri:	Mo. Rev. Stat. 407.010 *et seq.*;
Montana:	Mont. Code Ann. 30-14-101 *et seq.*;
Nebraska:	Neb. Rev. Stat. § 59-1601 *et seq.*;
Nevada:	Nev. Rev. Stat. 598.0903 *et seq.*;
New Hampshire:	N.H. Rev. Stat. 358-A:1 *et seq.*;
New Mexico:	N.M. Stat. Ann. 57-12-1 *et seq.*;
New Jersey:	N.J. Stat. Ann. 56:8-1 *et seq.*;
New York:	N.Y. Gen. Bus. Law 349 *et seq.*;

North Carolina:	N.C. Gen. Stat. 75-1.1 *et seq.*;
North Dakota:	N.D. Cent. Code 51-15-01 *et seq.*;
Ohio:	Ohio Rev. Code 1345.01 *et seq.*;
Oklahoma:	15 Okla. Stat. § 751 *et seq.*;
Oregon:	Or Rev. Stat. 646.605 *et seq.*;
Pennsylvania:	73 Pa. Stat. Ann. §§ 201-1 to -9.3 *et. seq.*;
Rhode Island:	R.I. Gen. Laws. 6-13.1-1 *et seq.*;
South Carolina:	S.C. Cod. Laws 39-5-10 *et seq.*;
South Dakota:	S.D. Cod. Laws 37-24-1 *et seq.*;
Tennessee:	Tenn. Code 47-18-101 *et seq.*;
Texas:	Tex. Bus. Com. Code 17.41 *et seq.*;
Utah:	Utah Code Ann. 13-5a-1 *et seq.*;
Vermont:	9 Vt. Stat. Ann. § 2451 *et seq.*;
Virginia:	Va. Code 59.1-196 *et seq.*;
Washington:	Wash. Rev. Code 19.86.010 *et seq.*;
West Virginia:	W. Va. Code 46A-6-101 et seq.;
Wisconsin:	Wis. Stat. 100.20 *et seq.*; and
Wyoming:	Wyo. Stat. 40-12-101 *et seq.*

95. Plaintiffs and the Class were injured by Defendants' conduct. As a direct and proximate result of Defendants' unfair methods of competition and unfair or deceptive acts or practices, Plaintiffs and the Class have suffered actual economic losses.

96. Defendants, through their acts of unlawful and unfair competition, have

wrongfully acquired money from Plaintiffs and the Class. Thus, Plaintiffs and the Class seek both monetary damages and to enjoin Defendants from continuing to violate the law.

97. Such conduct is ongoing and continues to this date. Plaintiffs and the Class are therefore entitled to the relief described herein.

98. Plaintiffs and the Class seek damages, together with appropriate exemplary damages, attorneys' fees, and costs of suit pursuant to the state statutes alleged herein.

FIFTH CAUSE OF ACTION
Fraudulent Concealment/Nondisclosure

99. The Plaintiffs hereby incorporate by reference each paragraph of this Complaint, as if fully set forth herein.

100. Defendants actively concealed from and failed to disclose to Plaintiffs and the Class the true defective nature of the Service.

101. Defendants were under a duty to Plaintiffs and the Class to disclose these facts because:

(a) Defendants are in a superior position to know the true character and quality of their Service, and the problems with the Service;

(b) Defendants made partial disclosures about the Service in their marketing and advertising and warranties, as alleged above, while not revealing their true character or quality of security; and

(c) Defendants actively concealed the nature of the defective Service.

102. The facts concealed by Defendants from Plaintiffs and the Class are material facts because any reasonable person would have considered those facts to be important in deciding whether or not to use the Service. Defendants intentionally concealed and failed to disclose the

true facts about the Service for the purpose of inducing Plaintiffs and the Class to choose and utilize the Service. Had Plaintiffs and the Class known of the defect in the Service they would not have chosen and utilized the Service on disclosed their financial information. As the result of Defendants' conduct, Plaintiffs and the class were harmed.

SIXTH CAUSE OF ACTION
Unjust Enrichment

103. The Plaintiffs hereby incorporate by reference each paragraph of this Complaint, as if fully set forth herein.

104. As a result of the deceptive and unfair sales and marketing practices outlined above, Plaintiffs and the Class were inadequately protected from ID theft and financial pilfering from third parties by Defendants' cheap and shoddy security hardware and non-existent computer security personnel.

105. The revenues flowing to Defendants from saving the cost of usual and adequate security measures inured to their benefit. Defendants have been enriched, at the expense of unwitting consumers, by profiting from the unconscionable practices described above.

106. Plaintiffs and the members of the Class, all of whom used Defendants' Service believing Defendants were providing adequate security of their financial data, have been damaged as a result of Defendants' actions, and the Defendants have been unjustly enriched thereby, by the savings of hundreds of thousands of dollars not spent to secure their data systems.

107. Plaintiffs and other members of the Class are entitled to damages as a result of the unjust enrichment of Defendants, including the disgorgement of all revenue received by Defendants as a result of this conduct.

SEVENTH CAUSE OF ACTION
Breach of Implied Covenant of Good Faith and Fair Dealing

108. Plaintiffs hereby incorporate by reference each paragraph of this Complaint, as if fully set forth herein.

109. Defendants have not provided Plaintiffs and the Class adequate compensation for losses described above. Defendants did not disclose the data breach of financial information to Card Holders sufficiently and timely. As such, some class members were fraudulently billed on credit cards stored with Defendants or by other means stemming from Defendants' acts or lack of action.

110. With this knowledge, Defendants did not act to cure their breach. Defendants engaged in improper business practices by failing to monitor or sufficiently offer adequate third party credit monitoring for no charge to the class members in a timely fashion. Defendants have acted to deprive Plaintiffs and the class of the benefits of their contracts. By these actions and those described above, Defendants breached their duty of good faith and fair dealing, Plaintiffs and the Class have been harmed by Defendants' actions.

JURY TRIAL DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury of all the claims asserted.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the proposed class members request that the Court enter an order or judgment against Defendants including the following:

A. Certification of the action under the Federal Rules of Civil Procedure and appointment of Plaintiffs as Class Representatives and their counsel of record as Class Counsel;

B. Damages in the amount of monies paid for to Citi for financial Services purported for online Security and fraud monitoring, and the cost of credit monitoring services provided by a third party;

C. Actual damages, statutory damages, punitive, or treble damages, and such other relief as provided by the statutes cited herein;

D. Prejudgment and post-judgment interest on such monetary relief;

E. Equitable relief in the form of restitution and/or disgorgement of all unlawful or illegal profits received by Defendants as a result of the unfair, unlawful, and/or deceptive conduct alleged herein;

F. Equitable relief in compensation for loss of use of Products and Services to Plaintiffs and members of the Class. Unless Defendants' unlawful practices are enjoined, Plaintiffs and the Class will continue to suffer irreparable injury; to this extent, their remedy at law is inadequate, and they are entitled to injunctive and other equitable relief herein requested;

G. The costs of bringing this suit, including reasonable attorneys' fees; and

H. All other relief to which Plaintiffs and members of the proposed Class may be entitled at law or in equity.

Dated: October 6, 2011

MURRAY FRANK LLP

Brian Murray (BM 9954)
275 Madison Avenue, Suite 801
New York, New York 10016
Tel: (212) 682-1818
Fax: (212) 682-1892

Attorneys for Plaintiff

Of Counsel:
Paul C. Whalen, Esq.